WATERMARKING METHODS, APPARATUSES, AND APPLICATIONS

(To provide a comprehensive disclosure without unduly lengthening the following specification, applicants incorporate by reference the cited patent documents.)

Watermarking is a quickly growing field of endeavor, with several different approaches. The present assignee's work is reflected in U.S. patents 5,710,834, 5,636,292, 5,721,788, allowed U.S. applications 08/327,426, 08/598,083, 08/436,134 (to issue as patent 5,748,763), 08/436,102 (to issue as patent 5,748,783), and 08/614,521 (to issue as patent 5,745,604), and laid-open PCT application WO97/43736. Other work is illustrated by U.S. patents 5,734,752, 5,646,997, 5,659,726, 5,664,018, 5,671,277, 5,687,191, 5,687,236, 5,689,587, 5,568,570, 5,572,247, 5,574,962, 5,579,124, 5,581,500, 5,613,004, 5,629,770, 5,461,426, 5,743,631, 5,488,664, 5,530,759,5,539,735, 4,943,973, 5,337,361, 5,404,160, 5,404,377, 5,315,098, 5,319,735, 5,337,362, 4,972,471, 5,161,210, 5,243,423, 5,091,966, 5,113,437, 4,939,515, 5,374,976, 4,855,827, 4,876,617, 4,939,515, 4,963,998, 4,969,041, and published foreign applications WO 98/02864, EP 822,550, WO 97/39410, WO 96/36163, GB 2,196,167, EP 777,197, EP 736,860, EP 705,025, EP 766,468, EP 782,322, WO 95/20291, WO 96/26494, WO 96/36935, WO 96/42151, WO 97/22206, WO 97/26733. Some of the foregoing patents relate to visible watermarking techniques. Other visible watermarking techniques (e.g. data glyphs) are described in U.S. patents 5,706,364, 5,689,620, 5,684,885, 5,680,223, 5,668,636, 5,640,647, 5,594,809.

Most of the work in watermarking, however, is not in the patent literature but rather in published research. In addition to the patentees of the foregoing patents, some of the other workers in this field (whose watermark-related writings can by found by an author search in the INSPEC database) include I. Pitas, Eckhard Koch, Jian Zhao, Norishige Morimoto, Laurence Boney, Kineo Matsui, A.Z. Tirkel, Fred Mintzer, B. Macq, Ahmed H. Tewfik, Frederic Jordan, Naohisa Komatsu, and Lawrence O'Gorman.

The artisan is assumed to be familiar with the foregoing prior art.

In the following disclosure it should be understood that references to watermarking encompass not only the assignee's watermarking technology, but can likewise be practiced with any other watermarking technology, such as those indicated above.

Watermarking can be applied to myriad forms of information. These include imagery (including video) and audio – whether represented in digital form (e.g. an image comprised of pixels, digital video, etc.), or in an analog representation (e.g. non-sampled music, printed imagery, banknotes, etc.) Watermarking can be applied to digital content (e.g. imagery, audio) either before or after compression. Watermarking can also be used in various "description" or "synthesis" language representations of content, such as Structured Audio, Csound, NetSound, SNHC Audio and the like (*c.f.* http://sound.media.mit.edu/mpeg4/) by specifying synthesis commands that generate watermark data as well as the intended audio signal. Watermarking can also be applied to ordinary media, whether or not it conveys information. Examples include paper, plastics, laminates, paper/film emulsions, etc. A watermark can embed a single bit of information, or any number of bits.

The physical manifestation of watermarked information most commonly takes the form of altered signal values, such as slightly changed pixel values, picture luminance, picture colors, DCT coefficients, instantaneous audio amplitudes, etc. However, a watermark can also be manifested in other ways, such as changes in the surface microtopology of a medium, localized chemical changes (e.g. in photographic emulsions), localized variations in optical density, localized changes in luminescence, etc. Watermarks can also be optically implemented in holograms and conventional paper watermarks.

One improvement to existing technology is to employ established web crawler services (e.g. AltaVista, Excite, or Inktomi) to search for watermarked content (on the Web, in internet news groups, BBS systems, on-line systems, etc.) in addition to their usual data collecting/indexing operations. Such crawlers can download files that may have embedded watermarks (e.g. *.JPG, *.WAV, etc.) for later analysis. These files can be processed, as described below, in real time. More commonly, such files are

queued and processed by a computer distinct from the crawler computer Instead of performing watermark-read operations on each such file, a screening technique can be employed to identify those most likely to be conveying watermark data. One such technique is to perform a DCT operation on an image, and look for spectral coefficients associated with certain watermarking techniques (e.g. coefficients associated with an inclined embedded subliminal grid). To decode spread-spectrum based watermarks, the analyzing computer requires access to the noise signal used to spread the data signal. In one embodiment, interested parties submit their noise/key signals to the crawler service so as to enable their marked content to be located. The crawler service maintains such information in confidence, and uses different noise signals in decoding an image (image is used herein as a convenient shorthand for imagery, video, and audio) until watermarked data is found (if present). This allows the use of web crawlers to locate content with privately-coded watermarks, instead of just publicly-coded watermarks as is presently the case. The queueing of content data for analysis provides certain opportunities for computational shortcuts. For example, like-sized images (e.g. 256 x 256 pixels) can be tiled into a larger image, and examined as a unit for the presence of watermark data. If the decoding technique (or the optional pre-screening technique) employs a DCT transform or the like, the block size of the transform can be tailored to correspond to the tile size (or some integral fraction thereof). Blocks indicated as likely having watermarks can then be subjected to a full read operation. If the queued data is sorted by file name, file size, or checksum, duplicate files can be identified. Once such duplicates are identified, the analysis computer need consider only one instance of the file. If watermark data is decoded from such a file, the content provider can be informed of each URL at which copies of the file were found.

Some commentators have observed that web crawler-based searches for watermarked images can be defeated by breaking a watermarked image into sub-blocks (tiles). HTML instructions, or the like, cause the sub-blocks to be presented in tiled fashion, recreating the complete image. However, due to the small size of the component sub-blocks, watermark reading is not reliably accomplished.

This attack is overcome by instructing the web-crawler to collect the display instructions (e.g. HTML) by which image files are positioned for display on a web page, in addition to the image files themselves. Before files collected from a web page are scrutinized for watermarks, they can be concatenated in the arrangement specified by the display instructions. By this arrangement, the tiles are reassembled, and the watermark data can be reliably recovered.

Another such postulated attack against web crawler detection of image watermarks is to scramble the image (and thus the watermark) in a file, and employ a Java applet or the like to unscramble the image prior to viewing. Existing web crawlers inspect the file as they find it, so the watermark is not detected. However, just as the Java descrambling applet can be invoked when a user wishes access to a file, the same applet can similarly be employed in a web crawler to overcome such attempted circumvention of watermark detection.

Although "content" can be located and indexed by various web crawlers, the contents of the "content" are unknown. A *.JPG file, for example, may include pornography, a photo of a sunset, etc.

Watermarks can be used to indelibly associate meta-data within content (as opposed to stored in a data structure that forms another part of the object, as is conventionally done with meta-data). The watermark can include text saying "sunset" or the like. More compact information representations can alternatively be employed (e.g. coded references). Still further, the watermark can include (or consist entirely of) a Unique ID (UID) that serves as an index (key) into a network-connected remote database containing the meta data descriptors. By such arrangements, web crawlers and the like can extract and index the meta-data descriptor tags, allowing searches to be conducted based on semantic descriptions of the file contents, rather than just by file name.

Existing watermarks commonly embed information serving to communicate copyright information. Some systems embed text identifying the copyright holder. Others embed a UID which is used as an index into a database where the name of the copyright owner, and associated information, is stored.

Looking ahead, watermarks should serve more than as silent copyright notices. One option is to use watermarks to embed "intelligence" in content. One form of intelligence is knowing its "home." "Home" can be the URL of a site with which the content is associated. A photograph of a car, for example, can be watermarked with data identifying the web site of an auto-dealer that published the image. Wherever the image goes, it serves as a link back to the original disseminator. The same technique can be applied to corporate logos. Wherever they are copied on the internet, a suitably-equipped browser or the like can decode the data and link back to the corporation's home page. (Decoding may be effected by positioning the cursor over the logo and pressing the right-mouse button, which opens a window of options – one of which is Decode Watermark.)

To reduce the data load of the watermark, the intelligence need not be wholly encoded in the content's watermark. Instead, the watermark can again provide a UID – this time identifying a remote database record where the URL of the car dealer, etc., can be retrieved. In this manner, images and the like become marketing agents – linking consumers with vendors (with some visual salesmanship thrown in). In contrast to the copyright paradigm, in which dissemination of imagery was an evil sought to be tracked and stopped, dissemination of the imagery can now be treated as a selling opportunity. A watermarked image becomes a portal to a commercial transaction.

(Using an intermediate database between a watermarked content file and its ultimate home (i.e. indirect linking) serves an important advantage: it allows the disseminator to change the "home" simply by updating a record in the database. Thus, for example, if one company is acquired by another, the former company's smart images can be made to point to the new company's home web page by updating a database record. In contrast, if the old company's home URL is hard-coded (i.e. watermarked) in the object, it may point to a URL that eventually is abandoned. In this sense, the intermediate database serves as a switchboard that couples the file to its current home.

The foregoing techniques are not limited to digital content files. The same approach is equally applicable with printed imagery, etc. A printed catalog, for

example, can include a picture illustrating a jacket. Embedded in the picture is watermarked data. This data can be extracted by a simple hand-scanner/decoder device using straightforward scanning and decoding techniques (e.g. those known to artisans in those fields). In watermark-reading applications employing hand-scanners and the like, it is important that the watermark decoder be robust to rotation of the image, since the catalog photo will likely be scanned off-axis. One option is to encode subliminal graticules (e.g. visualization synchronization codes) in the catalog photo so that the set of image data can be post-processed to restore it to proper alignment prior to decoding.

The scanner/decoder device can be coupled to a modem-equipped computer, a telephone, or any other communications device. In the former instance, the device provides URL data to the computer's web browser, linking the browser to the catalog vendor's order page. (The device need not include its own watermark decoder; this task can be performed by the computer.) The vendor's order page can detail the size and color options of the jacket, inventory availability, and solicit ordering instructions (credit card number, delivery options, etc.) – as is conventionally done with on-line merchants. Such a device connected to a telephone can dial the catalog vendor's toll-free automated order-taking telephone number (known, e.g., from data encoded in the watermark), and identify the jacket to the order center. Voice prompts can then solicit the customer's choice of size, color, and delivery options, which are input by Touch Tone instructions, or by voiced words (using known voice recognition software at the vendor facility).

In such applications, the watermark may be conceptualized as an invisible bar code employed in a purchase transaction. Here, as elsewhere, the watermark can serve as a seamless interface bridging the print and digital worlds

Another way of providing content with intelligence is to use the watermark to provide Java or ActiveX code. The code can be embedded in the content, or can be stored remotely and linked to the content. When the watermarked object is activated, the code can be executed (either automatically, or at the option of the user). This code can perform virtually any function. One is to "phone home" – initiating a browser and linking to the object's home. The object can then relay any manner of data to its home.

This data can specify some attribute of the data, or its use. The code can also prevent accessing the underlying content until permission is received. An example is a digital movie that, when double-clicked, automatically executes a watermark-embedded Java applet which links through a browser to the movie's distributor. The user is then prompted to input a credit card number. After the number has been verified and a charge made, the applet releases the content of the file to the computer's viewer for viewing of the movie. Support for these operations is desirably provided via the computer's operating system, or plug-in software.

Such arrangements can also be used to collect user-provided demographic information when smart image content is accessed by the consumer of the content. The demographic information can be written to a remote database and can be used for market research, customization of information about the content provided to the consumer, sales opportunities, advertising, etc.

In audio and video and the like, watermarks can serve to convey related information, such as links to WWW fan sites, actor biographies, advertising for marketing tie-ins (T-shirts, CDs, concert tickets). In such applications, it is desirable (but not necessary) to display on the user interface (e.g. screen) a small logo to signal the presence of additional information. When the consumer selects the logo via some selection device (mouse, remote control button, etc.), the information is revealed to the consumer, who can then interact with it.

Much has been written (and patented) on the topic of asset rights management. Sample patent documents include U.S. patents 5,715,403, 5,638,443, 5,634,012, 5,629,980. Again, much of the technical work is memorialized in journal articles, which can be identified by searching for relevant company names and trademarks such as IBM's Cryptolope system, Portland Software's ZipLock system, the Rights Exchange service by Softbank Net Solutions, and the DigiBox system from InterTrust Technologies.

An exemplary asset management system makes content available (e.g. from a web server, or on a new computer's hard disk) in encrypted form. Associated with the encrypted content is data identifying the content (e.g. a preview) and data specifying

various rights associated with the content. If a user wants to make fuller use of the content, the user provides a charge authorization (e.g. a credit card) to the distributor, who then provides a decryption key, allowing access to the content. (Such systems are often realized using object-based technology. In such systems, the content is commonly said to be distributed in a "secure container.")

Desirably, the content should be marked (personalized/serialized) so that any illicit use of the content (after decryption) can be tracked. This marking can be performed with watermarking, which assures that the mark travels with the content wherever -- and in whatever form -- it may go. The watermarking can be effected by the distributor – prior to dissemination of the encrypted object – such as by encoding a UID that is associated in a database with that particular container. When access rights are granted to that container, the database record can be updated to reflect the purchaser, the purchase date, the rights granted, etc. An alternative is to include a watermark encoder in the software tool used to access (e.g. decrypt) the content. Such an encoder can embed watermark data in the content as it is released from the secure container, before it is provided to the user. The embedded data can include a UID, as described above. This UID can be assigned by the distributor prior to disseminating the container. Alternatively, the UID can be a data string not known or created until access rights have been granted. In addition to the UID, the watermark can include other data not known to the distributor, e.g. information specific to the time(s) and manner(s) of accessing the content.

In other systems, access rights systems can be realized with watermarks without containers etc. Full resolution images, for example, can be freely available on the web. If a user wishes to incorporate the imagery into a web page or a magazine, the user can interrogate the imagery as to its terms and conditions of use. This may entail linking to a web site specified by the embedded watermark (directly, or through an intermediate database), which specifies the desired information. The user can then arrange the necessary payment, and use the image knowing that the necessary rights have been secured.

As noted, digital watermarks can also be realized using conventional (e.g. paper) watermarking technologies. Known techniques for watermarking media (e.g. paper, plastic, polymer) are disclosed in U.S. patents 5,536,468, 5,275,870, 4,760,239, 4,256,652, 4,370,200, and 3,985,927 and can be adapted to display of a visual watermark instead of a logo or the like. Note that some forms of traditional watermarks which are designed to be viewed with transmissive light can also show up as low level signals in reflective light, as is typically used in scanners. Transmissive illumination detection systems can also be employed to detect such watermarks, using optoelectronic traditional-watermark detection technologies known in the art.

As also noted, digital watermarks can be realized as part of optical holograms. Known techniques for producing and securely mounting holograms are disclosed in U.S. patents 5,319,475, 5,694,229, 5,492,370, 5,483,363, 5,658,411 and 5,310,222. To watermark a hologram, the watermark can be represented in the image or data model from which the holographic diffraction grating is produced. In one embodiment, the hologram is produced as before, and displays an object or symbol. The watermark markings appear in the background of the image so that they can be detected from all viewing angles. In this context, it is not critical that the watermark representation be essentially imperceptible to the viewer. If desired, a fairly visible noise-like pattern can be used without impairing the use to which the hologram is put.

Digital watermarks can also be employed in conjunction with labels and tags. In addition to conventional label/tag printing processes, other techniques – tailored to security – can also be employed. Known techniques useful in producing security labels/tags are disclosed in U.S. patents 5,665,194, 5,732,979, 5,651,615, and 4,268,983. The imperceptibility of watermarked data, and the ease of machine decoding, are some of the benefits associated with watermarked tags/labels. Additionally, the cost is far less than many related technologies (e.g. holograms). Watermarks in this application can be used to authenticate the originality of a product label, either to the merchant or to the consumer of the associated product, using a simple scanner device, thereby reducing the rate of counterfeit product sales.

Recent advances in color printing technology have greatly increased the level of casual counterfeiting. High quality scanners are now readily available to many computer users, with 300 dpi scanners available for under $100, and 600 dpi scanners available for marginally more. Similarly, photographic quality color ink-jet printers are commonly available from Hewlett-Packard Co., Epson, etc. for under $300.

Watermarks in banknotes and other security documents (passports, stock certificates, checks, etc. – all collectively referred to as banknotes herein) offer great promise to reduce such counterfeiting, as discussed more fully below. Additionally, watermarks provide a high-confidence technique for banknote authentication. One product enabled by this increased confidence is automatic teller machines that accept, as well as dispense, cash. The machine is provided with known optical scanning technology to produce digital data corresponding to the face(s) of the bill. This image set is then analyzed to extract the watermark data. In watermarking technologies that require knowledge of a code signal for decoding (e.g. noise modulation signal, crypto key, spreading signal, etc.), a bill may be watermarked in accordance with several such codes. Some of these codes are public – permitting their reading by conventional machines. Others are private, and are reserved for use by government agencies and the like. (*C.f.* public and private codes in the present assignee's issued patents.)

Banknotes presently include certain markings which can be used as an aid in note authentication. Well known visible structures are added to banknotes to facilitate visual authentication and machine detection. An example is the U.S. Federal Reserve seal. Others are geometrical markings. Desirably, a note is examined by an integrated detection system, for both such visible structures as well as the present watermark-embedded data, to determine authenticity.

The visible structures can be sensed using known pattern recognition techniques. Examples of such techniques are disclosed in U.S. Patents 5,321,773, 5,390,259, 5,533,144, 5,539,841, 5,583,614, 5,633,952, 4,723,149 and 5,424,807 and laid-open foreign application EP 766,449. The embedded watermark data can be recovered using the scanning/analysis techniques disclosed in the cited patents and publications.

To reduce counterfeiting, it is desirable that document-reproducing technologies recognize banknotes and refuse to reproduce same. A photocopier, for example, can sense the presence of either a visible structure *or* embedded banknote watermark data, and disable copying if either is present. Scanners and printers can be equipped with a similar capability – analyzing the data scanned or to be printed for either of these banknote hallmarks. If either is detected, the software (or hardware) disables further operation.

The watermark detection criteria provides an important advantage not otherwise available. An original bill can be doctored (e.g. by white-out, scissors, or less crude techniques) to remove/obliterate the visible structures. Such a document can then be freely copied on either a visible structure-sensing photocopier or scanner/printer installation. The removed visible structure can then be added in via a second printing/photocopying operation. If the printer is not equipped with banknote-disabling capabilities, image-editing tools can be used to insert visible structures back into image data sets scanned from such doctored bills, and the complete bill freely printed. By additionally including embedded watermark data in the banknote, and sensing same, such ruses will not succeed.

(A similar ruse is to scan a banknote image on a non-banknote-sensing scanner. The resulting image set can then be edited by conventional image editing tools to remove/obliterate the visible structures. Such a data set can then be printed – even on a printer/photocopier that examines such data for the presence of visible structures. Again, the missing visible structures can be inserted by a subsequent printing/photocopying operation.)

Desirably, the visible structure detector and the watermark detector are integrated together as a single hardware and/or software tool. This arrangement provides various economies, e.g., in interfacing with the scanner, manipulating pixel data sets for pattern recognition and watermark extraction, electronically re-registering the image to facilitate pattern recognition/watermark extraction, issuing control signals (e.g. disabling) signals to the photocopier/scanner, etc.

A related principle is to insert an imperceptible watermark having a UID into all documents printed with a printer, scanned with a scanner, or reproduced by a photocopier. The UID is associated with the particular printer/photocopier/scanner in a registry database maintained by the products' manufacturers. The manufacturer can also enter in this database the name of the distributor to whom the product was initially shipped. Still further, the owner's name and address can be added to the database when the machine is registered for warranty service. While not preventing use of such machines in counterfeiting, the embedded UID facilitates identifying the machine that generated a counterfeit banknote. (This is an application in which a private watermark might best be used.)

While the foregoing applications disabled potential counterfeiting operations upon the detection of *either* a visible structure or watermarked data, in other applications, both criteria must be met before a banknote is recognized as genuine. Such applications typically involve the receipt or acceptance of banknotes, e.g. by ATMs as discussed above.

The foregoing principles (employing just watermark data, or in conjunction with visible indicia) can likewise be used to prevent counterfeiting of tags and labels (e.g. the fake labels and tags commonly used in pirating Levis brand jeans, Microsoft software, etc.)

The reader may first assume that banknote watermarking is effected by slight alterations to the ink color/density/distribution, etc. on the paper. This is one approach. Another is to watermark the underlying medium (whether paper, polymer, etc.) with a watermark. This can be done by changing the microtopology of the medium (a la mini-Braille) to manifest the watermark data. Another option is to employ a laminate on or within the banknote, where the laminate has the watermarking manifested thereon/therein. The laminate can be textured (as above), or its optical transmissivity can vary in accordance with a noise-like pattern that is the watermark, or a chemical property can similarly vary.

Another option is to print at least part of a watermark using photoluminescent ink. This allows, e.g., a merchant presented with a banknote, to quickly verify the

presence of *some* watermark-like indicia in/on the bill even without resort to a scanner and computer analysis (e.g. by examining under a black light). Such photoluminescent ink can also print human-readable indicia on the bill, such as the denomination of a banknote. (Since ink-jet printers and other common mass-printing technologies employ cyan/magenta/yellow/black to form colors, they can produce only a limited spectrum of colors. Photoluminescent colors are outside their capabilities. Fluorescent colors – such as the yellow, pink and green dyes used in highlighting markers – can similarly be used and have the advantage of being visible without a black light.)

An improvement to existing encoding techniques is to add an iterative assessment of the robustness of the mark, with a corresponding adjustment in a re-watermarking operation. Especially when encoding multiple bit watermarks, the characteristics of the underlying content may result in some bits being more robustly (e.g. strongly) encoded than others. In an illustrative technique employing this improvement, a watermark is first embedded in an object. Next, a trial decoding operation is performed. A confidence measure (e.g. signal-to-noise ratio) associated with each bit detected in the decoding operation is then assessed. The bits that appear weakly encoded are identified, and corresponding changes are made to the watermarking parameters to bring up the relative strengths of these bits. The object is then watermarked anew, with the changed parameters. This process can be repeated, as needed, until all of the bits comprising the encoded data are approximately equally detectable from the encoded object, or meet some predetermined signal-to-noise ratio threshold.

The foregoing applications, and others, can generally benefit by multiple watermarks. For example, an object (physical or data) can be marked once in the spatial domain, and a second time in the spatial frequency domain. (It should be understood that any change in one domain has repercussions in the other. Here we reference the domain in which the change is directly effected.)

Another option is to mark an object with watermarks of two different levels of robustness, or strength. The more robust watermark withstands various types of

corruption, and is detectable in the object even after multiple generations of intervening distortion. The less robust watermark can be made frail enough to fail with the first distortion of the object. In a banknote, for example, the less robust watermark serves as an authentication mark. Any scanning and reprinting operation will cause it to become unreadable. Both the robust and the frail watermarks should be present in an authentic banknote; only the former watermark will be present in a counterfeit.

Still another form of multiple-watermarking is with content that is compressed. The content can be watermarked once (or more) in an uncompressed state. Then, after compression, a further watermark (or watermarks) can be applied.

Still another advantage from multiple watermarks is protection against sleuthing. If one of the watermarks is found and cracked, the other watermark(s) will still be present and serve to identify the object.

The foregoing discussion has addressed various technological fixes to many different problems. Exemplary solutions have been detailed above. Others will be apparent to the artisan by applying common knowledge to extrapolate from the solutions provided above.

For example, the technology and solutions disclosed herein have made use of elements and techniques known from the cited references. Other elements and techniques from the cited references can similarly be combined to yield further implementations within the scope of the present invention. Thus, for example, holograms with watermark data can be employed in banknotes, single-bit watermarking can commonly be substituted for multi-bit watermarking, technology described as using imperceptible watermarks can alternatively be practiced using visible watermarks (glyphs, etc.), techniques described as applied to images can likewise be applied to video and audio, local scaling of watermark energy can be provided to enhance watermark signal-to-noise ratio without increasing human perceptibility, various filtering operations can be employed to serve the functions explained in the prior art, watermarks can include subliminal graticules to aid in image re-registration, encoding may proceed at the granularity of a single pixel (or DCT coefficient), or may similarly treat adjoining groups of pixels (or DCT coefficients), the encoding can be optimized to

withstand expected forms of content corruption. Etc., etc., etc. Thus, the exemplary embodiments are only selected samples of the solutions available by combining the teachings referenced above. The other solutions necessarily are not exhaustively described herein, but are fairly within the understanding of an artisan given the foregoing disclosure and familiarity with the cited art.